**Amendments to the Specification:**

The Examiner objected to the specification because of a number of noted informalities. The Examiner is thanked for a very thorough review of the specification. Amendments to the specification addressing this objection are indicated herein. A copy of abstract is submitted. And a copy of substitute specification is submitted to incorporate the extensive amendments. The abstract and substitute specification includes no new matter.

Attachment: Abstract
Substitute Specification (Clean version and marked up version)

WO 2585-dV

TITLE OF THE INVENTION

Method for transferring data from a head-end to a number of receivers

BACKGROUND OF THE INVENTION

The present invention relates to a method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream.

The use of a digital broadcast signal, such as a DVB signal, for transferring data to one or more receivers shows the advantage that available receivers with descramblers can be used to transfer the data from a head-end to the receiver. However, such a method would normally not allow for a data transfer in a secure and private manner as the data is accessible to all receivers listening to the digital transport stream.

US-A-5 392 353 relates to an interactive satellite broadcast network, wherein encrypted communications ensure privacy of communications point-to-paint in a network of interactive video stations interconnected by a broadcast network. Although a broadcast network is mentioned, this document refers to-point-point communications. Personal identification keys are used known only by the individual participating stations and a secure single central switching control center. The network control center intercepts communications encrypted as a function of the senders personal identification key and relays incoming communications designating the receiver in encrypted format as a function of the receivers personal identification key.

US-A-5 432 850 relates to a method and apparatus for secure data transmission, wherein a plurality of data frames are transmitted, each containing at least an encrypted data sequence employing the destination address as at least part of a decryption key. At the receiver side,

the encrypted data sequence is decrypted by employing the local address of the receiver as at least part of the decryption key. In this known system each station can operate as a transmitting station using both the destination address and source address to encrypt the data.

EP-A-O 808 048 relates to a multimedia information service access, wherein a client can establish a connection with a server where desired multimedia information is resident. By selecting the desired multimedia information and providing a client information identifying this location of the user, the multimedia information is delivered by the server to a bridging apparatus through a switched network. It is indicated that the delivery of the multimedia information can be secured by comparing the client information to a segmented list to determine whether the client is authorized to receive the requested multimedia information.

The article "Internet Armor" by w. Stallings, Byte, vol. 21, no. 12, December *1996,* page 127-134, describes a method to provide secure IP package by encrypting the IP 'packet and providing a new IP header with the destination address. This document however relates to transfer data through the Internet.

## BRIEF SUMMARY OF THE INVENTION

The present invention provides a method of the above-mentioned type wherein privacy and security of the data transfer can be provided to each receiver.

According to the invention a method of the above-mentioned type is provided, including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets, scrambling said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled

transport packets of the digital transport stream only at the receiver having the unique key used to scramble the scrambled transport packets.

In this manner a method is obtained wherein each receiver attempting to descramble the broadcast signal will fail to descramble the signal except for the receiver(s) having the unique key(s) used to scramble the transport packets in which the data packets are inserted which are intended to be received by this receiver. This results in the desired privacy and security for the data transfer between the head-end and the receiver.

In a preferred embodiment for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being scrambled with a unique key corresponding with the individual address of the corresponding data packets.

In this manner data transfer with privacy and security is provided for a number of receivers requesting the transfer of data.

## BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The invention will be further explained by reference to the drawings in which an embodiment of the invention is schematically shown.

## DETAILED DESCRIPTION OF THE INVENTION

In this preferred embodiment the method is used to transfer data requested by a receiver from the Internet to the receiver on a digital broadcast signal or digital transport stream, so that an Internet connection is obtained with a high speed transfer of data to the receiver according to

the Internet Protocol. However the method described can also be used to transfer data to receivers at their request or initiated by the head-end in another manner.

In the drawing a DVB system is very schematically shown by way of example, the system comprising head-end equipment 1 which will be indicated hereinafter by head-end, and a large number of subscribers having a receiver 2, only one of which is shown in the drawing. The receiver 2 includes a descrambler 3 co-operating with a smart card 4 in a usual manner. The descrambler 3 is used to descramble DVB services requiring a subscription. The receiver 2 is connected to the Internet 5 in a manner not further shown, for example by a well-known modem. If the receiver 2 requests the download of data, the data will be transferred to the receiver 2 via the head-end 1 by means of a broadcast signal in the following manner.

According to the internet protocol the data includes an IP or MAC address of the receiver 2 requesting the data to be transferred to this receiver. Each receiver 2 for which the head-end 1 receives data packets with an individual address, i.e. the IP or MAC address, is sent a so-called Entitlement Control Message or ECM with a control word or key which is unique to the receiver 2. This message is encrypted using an individual key which is stored in the smart card 4. At the head-end 1 the unique keys with the corresponding individual addresses are stored in a table 6. At the receiver(s) 2 to which an ECM is sent, the smart card 4 decrypts the received message using its individual key to obtain the unique key. The decrypted key is loaded into the descrambler 3 for future use.

At the head-end 1, the data packets for a specific receiver 2 requesting the transfer of data, are inserted into transport packets of the digital transport stream. Generally, the data packets are larger than the transport stream packets, so that the data packets are split and thereafter inserted into a number of transport stream packets. Before scrambling the transport stream packets containing the data packets, the head-end checks the IP or MAC address and selects the corresponding unique key from the table 6, which key is used to scramble the transport stream packets.

Each receiver 2 to which the digital broadcast signal is transferred attempts to descramble the transport stream packets of the digital transport stream, wherein however only at the receiver 2 having the unique key used for scrambling the transport stream packets, the descrambling process will be successful. In this manner only one receiver 2 will descramble the scrambled transport stream packets to thereby obtain the IP data packets.

From the above it will be clear that the described method results in a transfer of data with privacy and security for each receiver 2 requesting a data transfer. Moreover, this transfer with privacy and security is achieved while using existing DVB or MPEG scrambling and descrambling equipment.

Generally, a number of receivers 2 will request the transfer of data. This is no problem as the head-end 1 will provide a table 6 including key/address combinations for each receiver 2 requesting a data transfer. The capacity of a digital broadcast signal is sufficient to transfer IP data packets to a large number of receivers 2. As the IP data packets for each particular receiver will be inserted into a number of transport packets wherein only these transport packets are scrambled using the unique key for this particular receiver, data transfer will still take place in a private and secure manner.

The data packets can be inserted into transport stream packets of a digital transport stream which is used for the transfer of data only. As an alternative the data packets can be inserted into transport stream packets of a DVB transport stream as the capacity of such a transport stream is far more than necessary for transferring the video information.

Although in the preferred embodiment the method is used to transfer IP data packets, the described method can also be used to transfer data from other sources than the Internet. Further, it is noted that instead of an ECM another type of message may be used to transfer a unique key to a receiver.